Защита данных и конфиденциальность


Мой папа говорит, что Facebook знает о нас всё
А он не твой папа

Защита персональных данных. Законы и требования

Требования по защите персональных данных в России существуют уже около 20 лет и с этого времени было выпущено большое количество различных документов и нормативных актов.

ФЗ 152 и персданные

Основным документом, определяющим необходимость защиты персональных данных в России является Федеральный закон РФ № 152-ФЗ «О персональных данных» вступивший в силу 26.01.2007. Этот документ определяет требования по работе с персональными данными (ПДн) российских граждан, обеспечивает защиту их интересов и надлежащий уровень такой защиты. Конечно, последний пункт вызывает некоторые сомнения, так как на практике утечки персональных данных стали, к сожалению, нормой. Но сейчас мы говорим лишь о правовой стороне вопроса.

Персональными данными будем называть любую информацию, которая относится к конкретному человеку, или субъекту персональных данных. ФИО, мобильный телефон, email, адрес проживания, фотография, паспортные данные — всё это ПДн. По сути, персональные данные эта та информация, по которой можно идентифицировать конкретного человека. Так, к примеру по фамилии имени и отчеству однозначно идентифицировать человека будет достаточно проблематично. Попробуйте в поисковике ввести чье-либо ФИО. Если обладатель имени, отчества или фамилии не имеет какие-то уникальные данные, то скорее всего вы получите несколько десятков двойников. Добавление населенного пункта не сильно улучшит ситуацию, так как для крупных городов также возможны совпадения. Добавление даты рождения с большой долей вероятности позволит однозначно идентифицировать субъекта персданных. Хотя и здесь бывали случаи, когда ГИБДД выписывали штрафы полным тезкам реальных нарушителей, из-за того, что у них совпадали ФИО и даты рождения, а проверкой других данных никто не удосужился. Таким образом, однозначным идентификатором субъекта могут быть его ФИО совмещенные с номером телефона, паспортными данными, СНИЛС и т.д.

Действующее российское законодательство предусматривает 4 категории обрабатываемых ПДн:

- общедоступные;
- биометрические;
- специальные;
- иные.

Закон о персональных данных с момента своего создания подвергался изменениям, однако, четко в нем прописаны только три первые группы, а вот в отношении “иных” нет особой конкретики.

И перед тем, как приступать к построению системы защиты персональных данных, операторам персданных необходимо понять, с какими сведениями они работают, и только потом устанавливать степень защищенности ИС.

Биометрические ПДн

К биометрическим персональным данным относятся фотографии, отпечатки пальцев, в более экзотических случаях это могут быть рисунки сетчатки глаза и т.д. Подобные физиологические идентификаторы субъекта входят в категорию биометрических ПДн.

Обработка таких персональных данных в обязательном порядке требует получения письменного согласия владельцев. Возможно, вы сталкивались с подобной практикой, когда при посещении какого-либо предприятия с вас сначала брали согласие на обработку персональных данных, а потом фотографировали на пропуск. Это частный случай обработки биометрии.

Работая с биометрией, оператору нужно брать в расчет ограничение по условиям обработки — их разрешено собирать, дополнять, хранить и т.д. только до тех пор, пока не достигнута цель обработки или не прошел срок, прописанный в подписанном субъектом разрешении. Здесь снова вспоминаем согласие на обработку ПДн, в нем должна быть четко указана цель обработки и сроки.

Специальная категория

Еще одним важным видом персональных данных, требующим серьезной защиты являются данные специальной категории. Это сведения, касающиеся состояния здоровья, гендерная и расовая принадлежность, сведения интимного характера, включая сексуальную ориентацию и все, что касается половой жизни, философские воззрения, религиозные убеждения, политические взгляды и т.д. Персональные данные специальной категории также требуют получение письменного согласия установленного законом образца.

При отсутствии письменного согласия оператор может использовать сведения специальной категории, если они опубликованы в общедоступных источниках самим гражданином, выполняются действия в рамках судебного производства или по решению суда, возникновение риска для жизни и здоровья субъекта либо окружающих людей, обработка информации в рамках деятельности общественной либо религиозной организации.

Иные ПДн

Как уже упоминалось ранее, в законе нет четкого определения, какие сведения могут быть отнесены в группу Иных, в нормативно-правовой документации нет. Указано только, что речь идет о ПДн, не относящихся к биометрии, специальной и общедоступным категориям. То есть оператору, чтобы идентифицировать информацию как «иную», придется убедиться в том, что она не является биометрической, общедоступной или специальной.

В категорию иных ПДн относят данные, которые не подпадают под остальные категории. В целом, эта категория самая распространённая и в неё входят ФИО, номер телефона, электронная почта, дата рождения и тому подобная информация. Пока такие данные не разместили в общедоступных источниках, они иные

То, что доступно всем

И еще одной достаточно распространенной категорией являются общедоступные. Это та информация, которая содержится в профилях в социальных сетях, на сайтах объявлений и других общедоступных ресурсах Интернет. Это может быть имя, фамилия, город проживания, телефон, электронная почта или личные фотографии. В этом случае оператором данных выступает владелец площадки, который обрабатывает данные о своих пользователях.

Уровень защищенности

Следующим шагом, который нам необходимо выполнить является установление уровня защищенности персональных данных. Под уровнем защищенности персональных данных (УЗ) понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

Здесь в игру вступает постановление Правительства №1119, которое устанавливает две категории субъектов персональных данных:

- лица, которые не являются штатными или внештатными сотрудниками организации;
- лица, связанные с компанией трудовыми взаимоотношениями.

Также, важную роль играет количество граждан, чьи ПДн обрабатываются — меньше или больше 100 000 субъектов. И наконец, постановление №1119 определяет типы актуальных угроз для ИСПДн.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Таблица 1. Определение уровней защищенности (УЗ) персональных данных

<table>
<tr><th rowspan="2">Категории ПДн</th><th rowspan="2">Сотрудники оператора</th><th rowspan="2">Количество субъектов</th><th colspan="3">Тип актуальных угроз</th></tr>
<tr><th>I (НДВ в СПО)</th><th>II (НДВ в ППО)</th><th>III (нет НДВ)</th></tr>
<tr><td rowspan="3">Специальные</td><td>Нет</td><td>более 100 000</td><td rowspan="4">УЗ-1</td><td>УЗ-1</td><td>УЗ-2</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td rowspan="3">УЗ-2</td><td rowspan="3">УЗ-3</td></tr>
<tr><td>Да</td><td>–</td></tr>
<tr><td>Биометрические</td><td>–</td><td>–</td></tr>
<tr><td rowspan="3">Общедоступные</td><td>Нет</td><td>более 100 000</td><td rowspan="3">УЗ-2</td><td rowspan="3">УЗ-4</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td>УЗ-3</td></tr>
<tr><td>Да</td><td>–</td></tr>
<tr><td rowspan="3">Иные</td><td>Нет</td><td>более 100 000</td><td rowspan="3">УЗ-1</td><td>УЗ-2</td><td>УЗ-3</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td rowspan="2">УЗ-3</td><td rowspan="2">УЗ-4</td></tr>
<tr><td>Да</td><td>–</td></tr>
</table>

Таблица 2. Определение требований, выполнение которых необходимо для обеспечения соответствующих УЗ

Требования	УЗ			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данные	+	+	+	+
Сохранность носителей персональных данных	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	–
Ограничение доступа к содержанию электронного журнала сообщений	+	+	–	–
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	–	–	–
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	–	–	–

Приказ ФСТЭК №21

Приказ ФСТЭК №21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”. Стоит отметить, что несмотря на то, что этому документу уже много лет, он до сих пор является одним из основных документов в части построения системы защиты.

Документ определяет пятнадцать групп различных технических и организационных мер, в каждой группе от 2 до 20 различных мер, напротив каждой меры отмечено, является ли эта мера базовой (то есть, по сути обязательной) для определенного уровня защищенности (если стоит плюс, то мера базовая, если нет — компенсирующая). Базовая мера является обязательной к исполнению, в то время как компенсирующая направлена на нейтрализацию актуальных угроз безопасности и применяются при невозможности технической реализации отдельных выбранных мер по обеспечению безопасности. Тут нужно заметить, что в перечне есть немало мер, которые могут быть только компенсирующими, то есть не отмечены плюсом ни для одного из четырех уровней защищенности.

Можно приступать к построению системы защиты. Такой алгоритм наших действий. Но вернемся к приказу 21. Вот эти 15 групп мер:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Ниже представлен список мер для первой группы ИАФ:

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+

Приказ ФСБ России от 10 июля 2014г. N378

Как известно, ФСТЭК регулирует требования к защитным механизмам в системах ИБ, за исключением криптографии. Требования к криптографии у нас регламентирует ФСБ и в части персональных данных таким регламентирующим документом является приказ №378. Данный приказ определяет состав и содержание мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты.

В зависимости от установленного уровня защищенности приказ определяет состав и содержание организационных и технических мер. Так, для 4 уровня защищенности выдвигаются требования к организации режима обеспечения безопасности помещений, в которых размещена информационная система, и криптографические средства защиты (СКЗИ), обеспечение сохранности носителей персональных данных и другие организационные и технические требования. Также выдвигаются требования к самим СКЗИ в зависимости от актуальности тех или иных угроз для ИСПДн.

Для используемых СКЗИ определены требования к используемому классу в зависимости от уровня защищенности и типа актуальных угроз. Определить соответствие классов СКЗИ можно с помощью следующей таблицы.

Уровень защищенности	Класс СКЗИ		
	АУ 1 типа	АУ 2 типа	АУ 3 типа
1	КА1	КВ2+	-
2	КВ2+	КВ2+	КС1+
3	-	КВ2+	КС1+
4	-	-	КС1+

Новая правовая реальность

Новый закон №420-ФЗ вводит понятие «оборотных» штрафов — санкции будут более серьёзными при повторных нарушениях. Закон требует, чтобы организации уведомляли Роскомнадзор об инцидентах в течение 24 часов с момента выявления утечки и в течение 72 часов сообщали о результатах внутренней проверки, что позволяет контролирующим органам оперативно реагировать на нарушения. Эти изменения, как официально заявлено, направлены на повышение ответственности компаний за защиту информации и стимулирование внедрения современных средств безопасности.

Новые требования охватывают практически все организации, которые обрабатывают персональные данные.

Каждая из этих структур обязана пересмотреть свои внутренние регламенты и усилить меры информационной безопасности, чтобы избежать возможных утечек и связанных с ними штрафов.

Новый закон устанавливает дифференцированную систему штрафов для юридических и должностных лиц в зависимости от масштабов утечки.

За утечку данных 1–10 000 человек или 10–100 000 уникальных идентификаторов:

- Юридические лица: 3–5 млн ₽
- Должностные лица: 200 000–400 000 ₽

За утечку данных 10–100 000 человек или от 100 000 до 1 млн уникальных идентификаторов:

- Юридические лица: 5–10 млн ₽
- Должностные лица: 300 000–500 000 ₽

За утечку данных более 100 000 человек или свыше 1 млн уникальных идентификаторов:

- Юридические лица: 10–15 млн ₽
- Должностные лица: 400 000–600 000 ₽

При этом распространение информации, включающей специальные категории персональных данных (например, биометрические данные), повлечёт штраф для юридических лиц до 15 млн ₽.
В случае повторных нарушений штрафы станут ещё строже: минимальный штраф для юридических лиц составит 20 млн ₽, а максимальный может достигнуть 500 млн ₽.

Проверка веб-сайта

1. Проверьте, какие данные вы собираете.

Начните с тщательного анализа всех данных, поступающих от пользователей. Важно понять, действительно ли вам необходим весь объём информации для нормальной работы сайта.

Закон требует минимизации сбора данных — это означает, что следует ограничиться только той информацией, которая непосредственно необходима для выполнения заявленных функций. Например, если на сайте собираются ФИО, контактные данные и другая личная информация, убедитесь, что каждый тип данных имеет законное основание для обработки и что пользователь дал на это явное согласие. Международный кодекс ICC/ESOMAR в разделе «Минимизация данных» рекомендует ограничивать сбор персональных данных только необходимыми для исследования сведениями, а Федеральный закон «О персональных данных» устанавливает, что обработка персональных данных должна проводиться с соблюдением этого принципа.

2. Обновите политику конфиденциальности и согласие на обработку данных.

Следующий шаг — пересмотреть и обновить документы, регулирующие обработку персональных данных. Политика конфиденциальности должна ясно и подробно описывать, какие данные собираются, для каких целей они используются и кому могут передаваться.

Важно, чтобы содержание документа соответствовало требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и чтобы в нём были отражены все изменения в порядке обработки данных, включая случаи трансграничной передачи информации, если вы на сайте используете, например, Google Analytics. Кроме того, необходимо обеспечить наличие актуальных форм согласия на обработку данных, где пользователь информирован о всех рисках и даёт своё согласие на обработку персональной информации.

3. Проверьте техническую защищённость сайта.

Уделите особое внимание защите данных на техническом уровне. Внедрите современные методы шифрования, такие как HTTPS и TLS/SSL, чтобы гарантировать безопасность данных при передаче между сервером и пользователями.

Регулярно обновляйте программное обеспечение и проводите тесты на проникновение, чтобы выявить и устранить потенциальные уязвимости. Не забудьте рассмотреть возможность внедрения многофакторной аутентификации, что также является эффективной мерой защиты.

4. Настройте логирование и мониторинг утечек.

Оперативное обнаружение и реакция на инциденты — ключевой элемент современной системы безопасности. Настройте систему логирования, которая будет фиксировать все критичные события, связанные с обработкой данных, а также внедрите систему мониторинга, способную оперативно сигнализировать о подозрительной активности. Как пример, интеграция с системами SIEM (Security Information and Event Management) помогает существенно сократить время реагирования на киберинциденты.

5. Проведите аудит хранения данных и распределите ответственность среди сотрудников.

Регулярный аудит — необходимое условие для соответствия требованиям нового законодательства. Проведите детальную проверку всех процессов, связанных с обработкой персональных данных (в том числе и хранением), чтобы убедиться, что они соответствуют установленным нормам. Важно не только выявить возможные слабые места, но и разработать план по их устранению. Назначьте ответственных сотрудников, которые будут курировать соблюдение мер безопасности, а также организуйте регулярное обучение персонала по вопросам защиты информации.

Основные причины утечек

Основная причина — человеческий фактор. А далее идут технические сбои и недостаточный контроль над процессами. Небрежность сотрудников, ошибки при настройке систем безопасности и использование устаревших технологий зачастую открывают злоумышленникам возможность получить доступ к конфиденциальной информации.

Например, в 2023 году одна из крупнейших онлайн-площадок — Ozon — столкнулась с утечкой данных, в результате которой информация миллионов пользователей, включая ФИО, контактные данные и адреса доставки, оказалась скомпрометированной. Этот инцидент вынудил весь сектор электронной коммерции пересмотреть меры защиты и оперативно обновить IT-инфраструктуру.

В том же 2022 Альфа-Банк подвергся кибератаке, связанной с уязвимостью в системе интернет-банкинга. Доступ злоумышленников к данным клиентов привёл к утечке информации о нескольких тысячах пользователей.

Еще один яркий пример — инцидент в МТС в 2023 году. Через незащищённый API злоумышленники получили доступ к информации сотен тысяч абонентов.

Большинство этих инцидентов обошлись компаниям в 60 000 рублей штрафа, но с мая 2025 года ситуация кардинально изменилась.

Д/з

1. Концепция 6Р
2. Защита данных с помощью криптографии
3. Электронная подпись